UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/484,691	01/18/2000	Hashem Mohammad Ebrahimi	1565.035US1	9980

21186 7590 06/08/2007
SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
06/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
09484691	1/18/2000	EBRAHIMI ET AL.	1565.035US1

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
Carl Colin	
ART UNIT	PAPER
2136	20070530

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

This is a Supplemental Examiner's Answer which includes the grounds of rejection of any claims missing in section 9 from the last Examiner's Answer mailed on 4/12/2007.

/CC/

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/484,691
Filing Date: January 18, 2000
Appellant(s): EBRAHIMI ET AL.

Joseph P. Mehrle
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed April 10, 2006 appealing from the Office action mailed November 11, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,401,125	MAKARIOS ET AL	6-2002
6,003,084	GREEN ET AL	12-1999
US 2002/0007317	CALLAGHAN ET AL	1-2002
5,805,803	BIRRELL ET AL	9-1998

6,728,884	LIM	4-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

9.1 **Claims 1-3, 7-8, 9-17, and 20-28** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,401,125 to **Makarios et al** in view of US Patent 6,003,084 to **Green et al**.

As per claim 1, Makarios et al substantially teaches a method for brokering state information exchanged between computers using at least one protocol above a transport layer, the method comprising the steps of: *receiving at a proxy a request from a client requesting a resource of an origin server wherein the transparent proxy is unknown to the client* (see column 4, lines 37 and column 4, lines 53-56) as interpreted by the Examiner, the proxy disclosed by **Makarios et al** meets the recitation of transparent proxy because the proxy is unknown to the client when the client sends the first request, the client sends the URL directly to a web server for HTTP objects (resource). **Makarios et al** discloses *redirecting the client request from the transparent proxy to* a signup web page that meets the recitation of *policy module* (column 4, lines 51-53 and column 5, lines 10-15); *obtaining at the transparent proxy policy enforcement data wherein the policy enforcement data is received from the policy module* (column 5, lines 15-27 and column 3, lines 1-10); a proxy cookie is generated in response to login information of the user and transmitting to the user to use as an authentication for further interactions with the proxy that meets the recitation of *generating at the proxy a policy state token in response to the policy enforcement data* (column 5, lines 10-24); *and transmitting the policy state token from the* *transparent proxy to the client wherein the policy state token is used as an authentication of the client to the transparent proxy for subsequent interactions between the client and the transparent proxy* (see column 5, lines 30-51). Although **Makarios et al** discloses the claimed method steps of claim 1, **Makarios et al** does not provide enough details on the architecture implemented in the invention regarding the policy module; it is interpreted by the Examiner that the policy module is a program running on the web proxy server, for example, the signup web page is part of the system (see column 5, lines 10-17 and column 2, lines 15-35). **Green et al** in an analogous art teaches a memory configured at least in part by a transparent proxy process, a processor for running the transparent proxy process, (see figure 1) at least one link for networked communication between the transparent proxy process, on the one hand, and a client computer and an origin server, on the other hand, for example (see figures 2 and 3); **Green et al** further teaches a secure transparent proxy that is transparent to both a client and a server (column 9, lines 5-12) and transmitting packets in accordance with a defined security policy (column 5, lines 25-30) having a security module to verify whether to grant or deny access to proxy services (column 7, line 48 through column 8, line 25 and column 9, line 12-67). **Green et al** discloses a transparent proxy comprising a connection manager and a security manager that meets the recitation of policy module residing within the same environment with the transparent proxy (see figure 3b and column 5, lines 34-40). In one embodiment, the proxy comprises a connection manager and a security manager that meets the recitation of policy module residing within the same environment with the transparent proxy (see figure 3b and column 5, lines 34-40), the proxy incorporates features of both application gateways and proxies to better serve client or the server depending on which side caused the firewall action to be triggered; and further discloses several advantages of the invention associated with the transparent proxy (column 5, lines 55 through column 6, line 20). **Green et al** discloses wherein policy enforcement data is received from the policy module because as the client transfers data request to the proxy, requesting information from a server, the proxy comprises modules and components wherein a connection manager operates with a security monitor which monitors the data from the client for conformance with predefined conditions and provides control information to the connection manager of the proxy which in turns controls the relay and directs it whether to establish connections to the server (see column 8, lines 14-25). In another embodiment, the proxy uses a filter component that also meets the recitation of policy module, and the filter component processes the policy enforcement data an returns status to the communication component of the proxy, based on the status, the proxy communicates accordingly to the server (see column 10, lines 28-47). Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to modify the invention of **Makarios et al** to implement some of the features of the inventive concept of **Green et al**, which provides a transparent proxy comprising security modules with more security and more versatility as taught by **Green et al**. One skilled in the art would have been motivated to do so because the transparent proxy disclosed by **Green et al** is transparent to both the client and the server, incorporating features of both application gateways and proxies, easy to configure, (see column 5, line 55 through column 6, line 20), it also provides more security and more versatility where additional filtering may be performed as desired, and it is associated with policy module that allows the proxy to use any defined protocols in accordance to defined security policy and provides transparency wherein no devices need to change any configuration information (column 9, lines 11-60).

As per claims 14-17, Makarios et al substantially teaches a method for brokering state information exchanged between computers using at least one protocol above a transport layer, the method comprising the steps of: *receiving at a proxy a request from a client requesting a resource of an origin server wherein the transparent proxy is unknown to the client* (see column 4, lines 37 and column 4, lines 53-56) as interpreted by the Examiner, the proxy disclosed by **Makarios et al** meets the recitation of transparent proxy because the proxy is unknown to the client when the client sends the first request, the client sends the URL directly to a web server for HTTP objects (resource). **Makarios et al** discloses *redirecting the client request from the transparent proxy to* a signup web page that meets the recitation of *policy module* (column 4, lines 51-53 and column 5, lines 10-15); *obtaining at the transparent proxy policy enforcement data wherein the policy enforcement data is received from the policy module* (column 5, lines 15-27 and column 3, lines 1-10); a proxy cookie is generated in response to login information of the user and transmitting to the user to use as an authentication for further interactions with the proxy that meets the recitation of *generating at the proxy a policy state token in response to the policy enforcement data* (column 5, lines 10-24); *and transmitting the policy state token from the transparent proxy to the client wherein the policy state token is used as an authentication of the client to the transparent proxy for subsequent interactions between the client and the transparent proxy* (see column 5, lines 30-51). Although **Makarios et al** discloses the claimed method steps of claim 1, **Makarios et al** does not provide enough details on the architecture implemented in the invention regarding the policy module; it is interpreted by the Examiner that the policy module is a program running on the web proxy server, for example, the signup web page is part of the system (see column 5, lines 10-17 and column 2, lines 15-35). **Green et al** in an analogous art teaches a memory configured at least in part by a transparent proxy process, a processor for running the transparent proxy process, (see figure 1) at least one link for networked communication between the transparent proxy process, on the one hand, and a client computer and an origin server, on the other hand, for example (see figures 2 and 3); **Green et al** further teaches a secure transparent proxy that is transparent to both a client and a server (column 9, lines 5-12) and transmitting packets in accordance with a defined security policy (column 5, lines 25-30) having a security module to verify whether to grant or deny access to proxy services (column 7, line 48 through column 8, line 25 and column 9, line 12-67). **Green et al** discloses a transparent proxy comprising a connection manager and a security manager that meets the recitation of policy module residing within the same environment with the transparent proxy (see figure 3b and column 5, lines 34-40). In one embodiment, the proxy comprises a connection manager and a security manager that meets the recitation of policy module residing within the same environment with the transparent proxy (see figure 3b and column 5, lines 34-40), the proxy incorporates features of both application gateways and proxies to better serve client or the server depending on which side caused the firewall action to be triggered; and further discloses several advantages of the invention associated with the transparent proxy (column 5, lines 55 through column 6, line 20). **Green et al** discloses wherein policy enforcement data is received from the policy module because as the client transfers data request to the proxy, requesting information from a server, the proxy comprises modules and components wherein a connection manager operates with a security monitor which monitors the data from the client for conformance with predefined conditions and provides control information to the connection manager of the proxy which in turns controls the relay and directs it whether to establish connections to the server (see column 8, lines 14-25). In another embodiment, the proxy uses a filter component that also meets the recitation of policy module, and the filter component processes the policy enforcement data an returns status to the communication component of the proxy, based on the status, the proxy communicates accordingly to the server (see column 10, lines 28-47). Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to modify the invention of **Makarios et al** to implement some of the features of the inventive concept of **Green et al**, which provides a transparent proxy comprising security modules with more security and more versatility as taught by **Green et al**. One skilled in the art would have been motivated to do so because the transparent proxy disclosed by **Green et al** is transparent to both the client and the server, incorporating features of both application gateways and proxies, easy to configure, (see column 5, line 55 through column 6, line 20), it also provides more security and more versatility where additional filtering may be performed as desired, and it is associated with policy module that allows the proxy to use any defined protocols in accordance to defined security policy and provides transparency wherein no devices need to change any configuration information (column 9, lines 11-60).

As per claims 2-3, Makarios et al discloses the limitation of receiving at the proxy a renewed request for the origin server resource, the renewed request containing the policy state token, wherein the renewed request contains the policy state token in a cookie in a header sent from the client to the proxy, for example (column 5, lines 25-32).

As per claims 7-8, Makarios et al teaches the limitation of wherein HTTP or HTTPS is a protocol used during at least one of the receiving and transmitting steps (column 3, lines 30-67).

As per claim 10, the combination of **Makarios et al** and **Green et al** teaches directory access protocol for authentication of client that meets the recitation of utilizing LDAP as a software to provide authentication information about the client and the transparent policy enforcement data obtained by the transparent proxy depends on the authentication thus provided (**Green et al,** column 9, lines 12-47). Therefore, claim 10 is rejected on the same rationale as the rejection of claim 1.

Claims 9 and 11 are similar to the rejected **claim 10** except for utilizing Novell Directory Services and SSL software respectively instead of LDAP. **Green et al** discloses other directory service protocols and any protocols used in X400's X500's. Therefore using NDS or SSL would have been obvious to one skilled in the art, as these protocols are well known. Therefore, claims 9 and 11 are rejected on the same rationale as the rejection of claim 1.

As per claim 12, Makarios et al. teaches the limitation of wherein the obtaining step extracts policy enforcement data from a redirection address field (see column 3, lines 1-10).

As per claim 13, Makarios et al. teaches the limitation of wherein the transmitting step transmits the policy state token in a cookie in a header sent from the proxy to the client (column 10-32).

As per claims 20-22, claim 20 adds another proxy with similar limitations as the rejected claim 14. To one with ordinary skilled in the art, the network can comprise of any number of clients and servers and adding more than one proxy to share some of the functions would have been a design choice and obvious to one skilled in the art because assigning proxies to handle specific functions or protocols is well known in the art.

Claims 23 and 28 recite some of the limitations found in claim 1 except for implementing the claimed method in a computer system and for using a first signal including a redirection command which specifies the policy module address as a redirection target (see **Makarios et al,** column 5, lines 10-25); and a second signal including a redirection command which specifies the transparent proxy server address as a redirection target (**Makarios et al,** column 5, lines 30-32). **Makarios et al** discloses a signup web page with an address that meets the recitation of policy module address. **Green and al** discloses the amended limitations of claim 23 as discussed in claim 1 above. Therefore, claims 23 and 28 are also rejected on the same rationale as the rejection of claim 1.

As per claim 24, Makarios et al teaches the limitation of wherein the first signal includes an identity broker address as the policy module address (see column 5, lines 10-25).

As per claim 25, Makarios et al teaches the limitation of wherein the first signal includes a login server address as the policy module address (see column 5, lines 10-25).

As per claim 26, Makarios et al teaches the limitation of wherein the second signal includes the policy enforcement data embedded in an address field with the transparent proxy server address (see column 5, lines 10-25).

Claims 27 is similar to the rejected **claim 1**, except for incorporating the claimed method of claim 1 into a computer medium. Therefore, claim 27 is rejected on the same rationale as the rejection of claim 1.

9.2 **Claims 4, 6, 18, 19, 29, and 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,401,125 to **Makarios et al** in view of US Patent 6,003,084 to **Green et al** as applied to claims 1-3 above and further in view of US Patent Publication US 2002/0007317 to **Callaghan et al.**

As per claim 4, Makarios et al discloses stripping in the proxy cookie to customize the client's information request as appropriate to the server (column 3, lines 1-10). **Callaghan et al.** in an analogous art teaches the step of forwarding to the origin server a portion of the renewed request, the forwarded portion omitting the policy state token (see page 6, paragraphs 88-90). **Callaghan et al.** further teaches in other embodiments the step of stripping off the state token (see page 4, paragraph 61 and page 5, paragraph 81). Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to modify the method as combined above to omit the policy state token when forwarding the request to server. One skilled in the art would have been motivated to do so because by omitting the policy state token the proxy can maintain the proxy cookie information secret to the server. The other advantage of adding and omitting state information as disclosed by **Callaghan et al** is that it enables a proxy to customize request and response as it fits to the proxy (page 4, paragraphs 61-62).

As per claim 6, Callaghan et al. teaches further comprising the steps at the proxy of forwarding to the client at least a portion of a communication from the origin server, and forwarding to the origin server at least a portion of a communication from the client (page 5, paragraphs 81-82). Therefore, claim 6 is rejected on the same rationale as the rejection of claim 4.

Claim 18 recites some of the limitations of claims 1 and 4 as discussed above. For instance, **Green et al** discloses transparent proxy service that is transparent to both client and server, the combined references above also teach the step of accepting the authorization from the client with a renewed client request for the origin server resource; forwarding the renewed client request to the origin server without forwarding the authorization but with an indication to the origin server that the transparent proxy server is the source of the forwarded request, and then transparently forwarding the requested resource from the origin server to the client as mentioned in claims 1 and 4. Therefore claim 18 is rejected on the same rationale as the rejection of claims 1 and 4.

As per claim 19, Makarios et al teaches the limitation of wherein the transparent proxy server sends the client the authorization by sending the client a proxy cookie for use in subsequent communications from the client, for example (see column 5, lines 19-51).

Claims 29 and 30 recite some of the limitations found in claim 18, therefore they are rejected on the same rationale as the rejection of claim 18.

9.3 **Claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,401,125 to **Makarios et al** in view of US Patent 6,003,084 to **Green et al,** in view of US Patent Publication US 2002/0007317 to **Callaghan et al** as applied to claim 4 above and further in view of US Patent 5,805,803 to **Birrell et al.**.

As per claim 5, Makarios et al discloses an example of reply containing an origin state token for use by the proxy in its subsequent communications with a (column 5, lines 55-65). It is obvious to one skilled to the art that the same concept can be applied in the server side (see figure 2) as the proxy is capable of saving the cookie for future interactions with the server. **Green et al** discloses transparency with both the server and the client and discloses interaction between the proxy and the server (column 11, lines 5-17). **Birrell et al.** in an analogous art discloses receiving at the proxy a reply from the origin server, the reply containing an origin state token for use by the proxy in its subsequent communications with the origin server, for example (see column 4, lines 51-65). Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to modify the method as combined above to include the step of receiving at the proxy a reply from the origin server, the reply containing an origin state token for use by the proxy in its subsequent communications with the origin server. One skilled in the art would have been motivated to do so because using the origin state token for use by the proxy in its subsequent communications with the origin server will allow the proxy to save in time and bandwidth if the server is already known to the server rather than authenticating at every session (column 4, lines 51-65 and 13-26).

9.4 **Claim 31** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,401,125 to **Makarios et al** in view of US Patent 6,003,084 to **Green et al** as applied to claim 27 above and further in view of US Patent Publication US Patent 6,728,884 to **Lim**.

As per claim 31, both references substantially teach the step of generating at the proxy a policy state token in response to the policy enforcement data (**Makarios et al**, column 5, lines 19-51); transmitting the policy state token from the proxy to the client (**Makarios et al**, column 5, lines 19-51); receiving the proxy cookie from the client with a renewed client request for the origin server resource (**Makarios et al**, column 5, lines 19-51), and redirecting client request from a transparent proxy to a policy module and accepting the policy enforcement data (**Makarios et al**, column 5, lines 19-51). Neither of the references explicitly teach redirecting a request from a <u>second</u> transparent proxy to be to, and accepting the policy enforcement data at the second transparent proxy. To a person skilled in the art it is apparent that the proxy disclosed by the combined references above can be implemented in more than one computer to obtain a second transparent proxy that will perform the same function. Load balancing is well known in the art; and in load balancing, another transparent proxy or gateway can perform a specific function when the first one is not available. **Lim** in an analogous art teaches a plurality of proxy servers associated with several security modules to control and provide access to resources (column 3, lines 40-57). **Lim** discloses proxy configuration data that specifies the configuration of each proxy servers; the proxy configuration data specifies whether a particular proxy security server provides authorization services (column 6, line 65 through column 7, line 5) and discloses request can be received by a specific proxy server since the request may include data that indicates which proxy servers to use and further discloses proxy server requests security module (column 5, lines 60-67 and column 6, lines 15-20); a returned cookie is required for access to resources (column 6, lines 34-35) and further discloses that not all the proxies may provide the same set of services a service may be available for a specific service while another server provides that particular service (column 8, lines 59-67) that meets the recitation of accepting at the second transparent proxy the second policy enforcement data provided by the policy module, the second policy enforcement data including authorization from the policy module for the client to access the resource through the second transparent proxy. Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to modify the method as combined above to include a second transparent proxy where a request can be received after the first proxy becomes unavailable and accepting at a second proxy policy enforcement data from policy module for authorization to access resources as suggested by **Lim**.

One skilled in the art would have been motivated to utilize more than one proxy because it provides the advantage of governing access to more information resources and selective proxies can be assigned to specific security policies and if there is a need for reconfiguration other proxies will be available (see column 2, lines 27-36) as suggested by **Lim**.

(10) Response to Argument

Appellant's statements on the grounds of rejection are not correct. The issues raised by Appellant were fully responded under the grounds of rejection. Appellant argues that Makarios teaches away from a transparent proxy. Examiner's interpretation of a transparent proxy is correctly, reasonably, and broadly interpreted in light of Applicant's specification. For instance, Applicant's specification page 8, lines 19 - page 9, line 2 cites,

> "A given transparent proxy B will not necessarily recognize client A which is making the request, if earlier requests from client A were serviced by a different proxy or if this is the first request to the origin web server X. In order for the current proxy B to establish, retrieve, and maintain state, the invention uses state tokens in the form of transparent proxy cookies. First, B examines the HTTP request that it receives from client A for an object R on the origin server X, and determines that the request does not contain a proxy cookie meeting the intranet policy requirements."

As noted above, a transparent proxy will not necessarily recognize client A if this is the first request to the origin web server X. A transparent proxy receives request from client A for an object on the origin server X and determines if the request contains a proxy cookie conforming to a policy requirement.

Makarios et al reference column 4, lines 31-37 and lines 53-59 cites,

> "As shown in FIG. 3, in Step 100 the system (preferably a computer program running on the proxy 20 or something similar) monitors requests generated by the browser client 10 for HTTP objects. When the browser client 10 generates such a request, it is intercepted and in Step 110 the system checks it to see if it contains a proxy cookie 50', i.e., a cookie conforming to a special format such as

> perucookie=<userID>;"
>
> "Assume, for example, in Step 100 the browser client initially requests an HTTP object such as a web page as follows:
> GET http://www.bungalow.com
> Seeing no proxy cookie 50' in Step 110, in Step 120 the proxy 20 would redirect the browser client 10, causing it in Step 130 to generate the subsequent information request".

Therefore, Examiner's interpretation is correct. Makarios et al meets the claimed limitation as claimed. The proxy is transparent to the client because the proxy intercepts HTTP request destined for an Internet server and determines if the request contains a proxy cookie conformed to a special format (policy requirement). The proxy is unknown to the client when making the first request: "GET http://www.bungalow.com" and no proxy cookie is present. In addition, interaction between the client and the proxy is performed above without the client initially configured or registered with the proxy contrarily to appellant's argument (see appellant's brief page 11, lines 1-4).

Applicant further argues that the client of Makarios must not only be aware of the proxy but must register with the proxy and because a user of the client must provide a username the proxy of Makarios is not transparent. Examiner respectfully disagrees. First as explained clearly above, the client of Makarios et al was not aware of the proxy, therefore the proxy must be transparent. Second, in response to Appellant's argument that in Makarios "the user of the client must provide a handle or username before interaction with that proxy can commence see Makarios col. 5, lines 10-17," it is noted that (steps 140-150) cited herein by Appellant are not executed before interaction with the proxy can commence, there was already interaction with the proxy in steps 110-130 as it will be shown below. (See also Makarios et al, claim 1).

Appellant's argument regarding the client of Makarios is redirecting to a signup web page to provide a user ID for identification (see Makarios figure 4) for showing that the proxy is not transparent, is contradictory to the specification and the claimed invention because the claimed invention requires the same: a step of "redirecting the client request from the transparent proxy to a policy module" and a step of "obtaining at the transparent proxy policy enforcement data (login information), wherein the policy module and the transparent proxy reside within a same environment." Applicant's specification page 9, lines 1-13 describes, (note B is the transparent proxy and A is the client),

> "First, B examines the HTTP request that it receives from client A for an object R on the origin server X, and determines that the request does not contain a proxy cookie meeting the intranet policy requirements."
>
> "B therefore formats an A-B-I state token appended to or otherwise embedded in the redirection target address, and **redirects A to an identity broker I** along with relevant request data appended to the identifier or otherwise attached to the HTTP redirect command. That is, B uses the conventional HTTP redirect facility to redirect the request to a possibly novel target, and B may use familiar techniques to append or embed data into an URL or URI to place novel proxy cookie data in the command with the target address. Identity broker I extracts or otherwise separates the A-B-I state token from the address or request header, verifies B's credentials, and uses the HTTP redirect facility to **redirect A to a login service L that can validate A's identity** and give it authorization to use the network. The login server L redirects A's request back to the identity broker I after A successfully logs in (note that proxy B, identity broker I, and login service L can all be running on the same machine).

That is in Applicant's specification, the client is redirected to a login service residing at the transparent proxy and user validation is performed at the transparent proxy.

Makarios et al, column 4, lines 49-67 cites redirecting the client request as claimed and further discloses redirecting the client request when no proxy cookie is present:

> "If, on the other hand, Step 110 determines that no proxy cookie 50' was included with the information request from the browser client 10, in Step 120 the proxy 20 will cause the browser client 10 to redirect to a new web page in a manner known in the art. Assume, for example, in Step 100 the browser client initially requests an HTTP object such as a web page as follows:
>
> GET http://www.bungalow.com
>
> Seeing no proxy cookie 50' in Step 110, in Step 120 the proxy 20 would redirect the browser client 10, causing it in Step 130 to generate the subsequent information request

> GET http://peru.host/ ?peru-command=peru-fetch-peru-cookie&peru-url=http%3A%2F%2Fwww.bungalow.com%2F
> where peru.host is a syntactically valid (albeit fictitious) URL and peru-command=perufetch-peru-cookie and peru-url=http%3A%2F%2Fwww.bungalow.com%2F are fields which the proxy 20 has directed the browser client 10 to include in the request."

Makarios et al further discloses determining and asking the user for login information after a <u>second</u> request, (a redirection request); not before interaction with the proxy can commence, as argued by Appellant:

> Having received the product of the redirection from the browser client 10 in Step 130, in Step 140 the system examines the redirected request to see if the browser client 10 has also included a cookie for peru.host, i.e., perucookie=<userID>;. If Step 140 determines that the latter is the case, i.e., this is the first time for the user to access the proxy 20 from this browser client 10, in Step 150 the system serves the browser client 10 a signup web page or form as prompting him or her to provide a handle or nickname for identification in subsequent transactions, as shown in FIG. 4. Simultaneously, in Step 150 the system directs the browser client 10 to store a proxy cookie 50' which appears to come from the peru. host domain. When the user types in a name and submits the form, the name is returned to the proxy 20 (along with the proxy cookie 50', since it now matches the peru.host domain). Then, in Step 160, proxy 20 stores the name for this user, associated with the proxy cookie 50', for use in future customization operations. (see column 5, lines 1-5 and 10-25)

On page 13, lines 7-9 appellant argues that "Makarios is heavily reliant on a forward proxy arrangement and requires direct client registration and configuration to establish the initial cookie for a user on the client that the client than actively attaches to requests and forwards to the proxy". For the sake of argument, it is noted that Appellants's specification discloses the same for instance, on page 10, lines 2-5, after client A provides identification information and is being validated:

> "B responds with a another redirection, for exactly the same resource, and this redirection contains the valid A-B-X state token in its header as a proxy cookie. It is important to note that because B is a proxy, it can send cookies that A will use when requesting.resources from X. A then re-requests the resource from X, this time with the proxy cookie required by B contained in the request header."

As explained in the Response to Argument above, Makarios et al discloses a transparent proxy, therefore, Appellant's arguments that Makarios et al cannot be combined to Green because Makarios does not disclose a transparent proxy is not correct. The claims have been combined in the Final rejection dated 11/3/2005 not because the proxy of Makarios et al is not transparent but to clearly disclose the functions of the policy module and more specifically to clearly disclose the additional features of claim 14 with respect to the architecture of a transparent proxy server that includes a policy module.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Carl Colin/
Examiner, A.U. 2136
May 30, 2007

Conferees:

Eddie Lee

EDDIE C. LEE
SUPERVISORY PATENT EXAMINER

Taghi Arani

Novell INC.
1800 SOUTH NOVELL PLACE
PROVO, UTAH 84606